

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION**

QUICKVAULT, INC.,

Plaintiff,

v.

BROADCOM INC., d/b/a BROADCOM
CORPORATION

Defendant.


Case No.: 1:24-cv-00864

JURY TRIAL DEMANDED

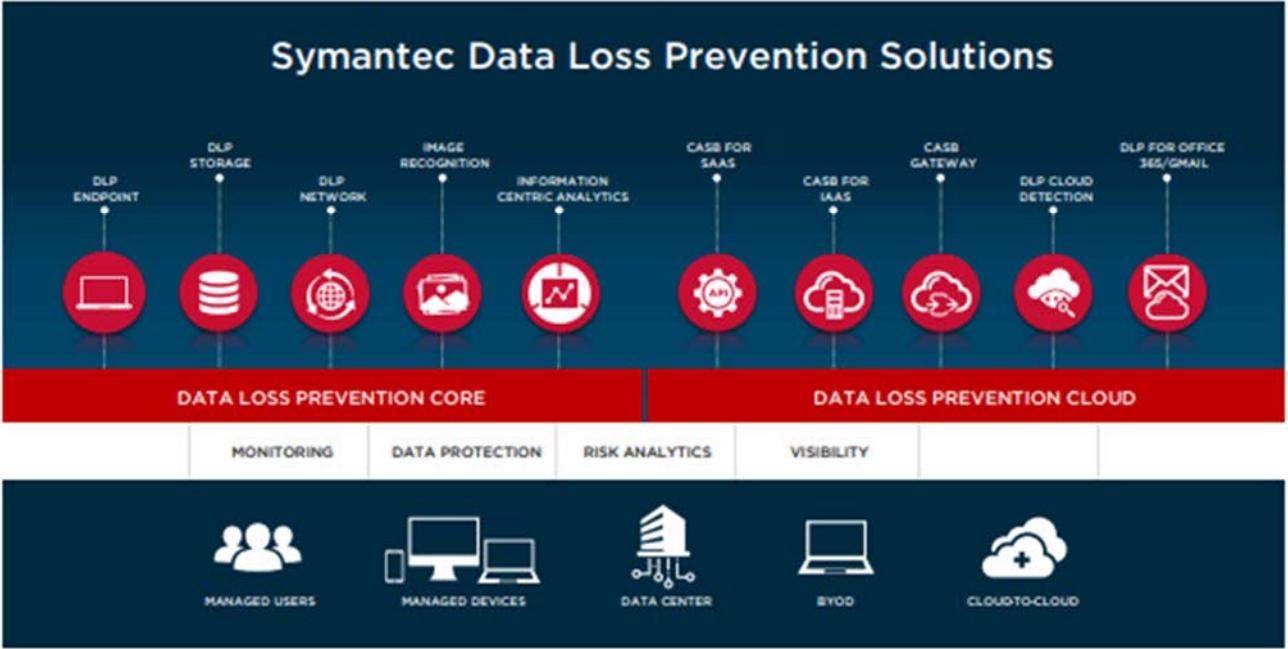
EXHIBIT J

'300 Patent Infringement Claim Chart

EXHIBIT J: U.S. PATENT NO. 10,999,300 INFRINGEMENT CLAIM CHART¹

Claim 1	Symantec Enterprise Cloud
A forensic computing platform deployed as a cloud control server which comprises	<p>The preamble is presumptively not limiting. To the extent the preamble is limiting, Symantec Enterprise Cloud is a forensic computing platform deployed as a cloud control server.</p> <p>Symantec Enterprise Cloud Buy via Partner</p>  <p>Symantec Enterprise Cloud delivers data-centric hybrid security for the largest, most complex organizations in the world – on devices, in private data centers, and in the cloud.</p> <ul style="list-style-type: none"> • Consistent Compliance: Apply and manage compliance controls consistently across the infrastructure. • Secure Remote Work: Protect critical enterprise assets wherever they live and from wherever they are accessed. • Data and Threat Protection Everywhere: Unify intelligence across control points to detect, block, and remediate targeted attacks.

¹ The evidence of infringement identified in the below chart is exemplary and nonlimiting. QuickVault reserves the right to rely on additional and/or alternative aspects of Symantec Enterprise Cloud and related components during this litigation for the purpose of establishing infringement.

Claim 1	Symantec Enterprise Cloud
	<p>(https://www.broadcom.com/products/cybersecurity)</p>  <p>The diagram illustrates the Symantec Data Loss Prevention Solutions architecture. It is divided into two main horizontal sections: 'DATA LOSS PREVENTION CORE' and 'DATA LOSS PREVENTION CLOUD'. The CORE section includes components like DLP ENDPOINT, DLP STORAGE, DLP NETWORK, IMAGE RECOGNITION, INFORMATION CENTRIC ANALYTICS, CASB FOR SAAS, CASB FOR IAAS, CASB GATEWAY, DLP CLOUD DETECTION, and DLP FOR OFFICE 365/GMAIL. These are supported by a foundation of MONITORING, DATA PROTECTION, RISK ANALYTICS, and VISIBILITY. The CLOUD section includes MANAGED USERS, MANAGED DEVICES, DATA CENTER, BYOD, and CLOUD-TO-CLOUD.</p> <p>(https://docs.broadcom.com/doc/data-loss-prevention-family-en.)</p>

Claim 1	Symantec Enterprise Cloud						
an analytic component,	<p data-bbox="617 289 1577 347">About scanning targeted endpoints</p> <p data-bbox="617 363 930 391">Last Updated May 3, 2024</p> <p data-bbox="617 435 1394 462">You can use targeted Endpoint Discover scans to do the following:</p> <ul data-bbox="617 483 1848 657" style="list-style-type: none"> • Define an Endpoint Discover scan that uses multiple Endpoint Servers to target endpoints. • Define an Endpoint Discover scan that targets individual endpoints. An Endpoint Discover Target can be configured to scan specific endpoints. You can identify the endpoints using host name or IP address. You can also upload a file that lists endpoints by host name and IP address. Scan policies are applied only on these specified endpoints. <p data-bbox="617 678 1041 706">Creating an Endpoint Discover scan</p> <p data-bbox="617 727 1818 787">You can use one of the following options as described in the following table when creating an Endpoint Discover Target:</p> <p data-bbox="617 841 1184 868">Options for creating an Endpoint Discover target</p> <table data-bbox="617 885 1875 1382"> <thead> <tr> <th data-bbox="617 885 814 966">Option</th><th data-bbox="814 885 1875 966">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="617 982 814 1187">Specify the Endpoint Servers without specifying the endpoints</td><td data-bbox="814 982 1875 1084">In this case, the Enforce Server sends the scan details to the specified Endpoint Servers. When the endpoints connect to the specified Endpoint Servers, then the scan details are sent to them.</td></tr> <tr> <td data-bbox="617 1235 814 1382">Specify the Endpoint Servers and the endpoints</td><td data-bbox="814 1235 1875 1382">In this case, the Enforce Server sends the scan details to the specified Endpoint Servers. When the specified endpoint connects to the specified Endpoint Server, the scan details are sent to the specified endpoints. Thus, only the specified endpoints run the scan, and optimize the network bandwidth and save time.</td></tr> </tbody> </table>	Option	Description	Specify the Endpoint Servers without specifying the endpoints	In this case, the Enforce Server sends the scan details to the specified Endpoint Servers. When the endpoints connect to the specified Endpoint Servers, then the scan details are sent to them.	Specify the Endpoint Servers and the endpoints	In this case, the Enforce Server sends the scan details to the specified Endpoint Servers. When the specified endpoint connects to the specified Endpoint Server, the scan details are sent to the specified endpoints. Thus, only the specified endpoints run the scan, and optimize the network bandwidth and save time.
Option	Description						
Specify the Endpoint Servers without specifying the endpoints	In this case, the Enforce Server sends the scan details to the specified Endpoint Servers. When the endpoints connect to the specified Endpoint Servers, then the scan details are sent to them.						
Specify the Endpoint Servers and the endpoints	In this case, the Enforce Server sends the scan details to the specified Endpoint Servers. When the specified endpoint connects to the specified Endpoint Server, the scan details are sent to the specified endpoints. Thus, only the specified endpoints run the scan, and optimize the network bandwidth and save time.						

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="598 266 1848 373">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-network-discover-scanning/about-scanning-targeted-endpoints.html)</p> <h2 data-bbox="598 397 1659 454">About Endpoint Discover full scanning</h2> <p data-bbox="598 470 924 503">Last Updated May 3, 2024</p> <p data-bbox="598 544 1885 609">An Endpoint Discover Target can be configured to use the full scan option. This option scans all the files on the endpoint.</p> <p data-bbox="598 625 1848 690">If you have changed the policy or modified the filters significantly in an existing endpoint target and want these changes to take effect, then you may need to run a full scan instead of an incremental scan.</p> <p data-bbox="598 722 1848 836">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-network-discover-scanning/about-endpoint-discover-full-scanning.html)</p>

Claim 1	Symantec Enterprise Cloud
a reporting component,	<h2 data-bbox="604 289 1350 349">Setting Report Preferences</h2> <p data-bbox="604 365 995 394">Last Updated February 16, 2024</p> <p data-bbox="604 435 1808 500">You can specify your preferences for the reports that Symantec Data Loss Prevention displays in the navigation panel for each of the report types.</p> <ol data-bbox="617 521 1675 597" style="list-style-type: none"> <li data-bbox="617 521 1675 553">1. In the Enforce Server administration console, on the Incidents menu, click All Reports. <li data-bbox="617 565 1241 597">2. On the All Reports screen, click Edit Preferences. <p data-bbox="646 621 1877 686">The Edit Report Preferences screen lists any saved reports (for all your assigned roles). The screen also lists Network, Endpoint, Discover, and Applications (Cloud and API Appliance) reports.</p> <ol data-bbox="617 711 1850 776" style="list-style-type: none"> <li data-bbox="617 711 1850 776">3. To display a report in the list, check the Show Report box for that report. To remove a report from the list, clear the Show Report box for that report. <p data-bbox="646 800 1751 865">The selected list of reports displays in a left navigation panel for each of the types of reports. For example, to see the list of Network reports, on the Incidents menu, click Network.</p> <ol data-bbox="617 889 785 922" style="list-style-type: none"> <li data-bbox="617 889 785 922">4. Click Save. <p data-bbox="596 954 1850 1060">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/Incidents/managing-and-reporting-incidents/setting-report-preferences-id-sf0b0127086-d336e1191.html)</p>

About Incident Reports

Last Updated February 16, 2024

Use incident reports to track and respond to incidents on your network. Symantec Data Loss Prevention reports an incident when it detects data that matches a detection rule in an active policy. Such data may include specific file content, an email sender or recipient, attachment file properties, or many other types of information. Each piece of data that matches a detection rule is called a match, and a single incident may include any number of individual matches.

Note

To configure which reports appear in the navigation panel, go to **All Reports** and click **Edit Preferences**.

Symantec Data Loss Prevention provides the following types of incident reports:

Incident lists	These show individual incident records containing information such as severity, associated policy, number of matches, and status. You can click on any incident to view a snapshot containing more details. You can select specific incidents or groups of incidents to modify or remediate.
Summaries	These show incident totals organized by a specific incident attribute such as status or associated policy. For example, a Policy Summary includes rows for all policies that have associated incidents. Each row includes a policy name, the total number of associated incidents, and incident totals by severity. You can click on any severity total to view the list of relevant incidents.
Double summaries	These show incident totals organized by two incident attributes. For example, a policy trend summary shows the total incidents by policy and by week. Similar to the policy summary, each entry includes a policy name, the total number of associated incidents, and incident totals by severity. In addition, each entry includes a separate line for each week, showing the week's incident totals and incidents by severity.

Claim 1	Symantec Enterprise Cloud
	<p>Dashboards and executive summaries</p> <p>These are quick-reference dashboards that combine information from several reports. They include graphs and incident totals representing the contents of various incident lists, summaries, and double summaries. Graphs are sometimes beside lists of high-severity incidents or lists of summary groups. You can click on constituent report names to drill down to the reports that are represented on the dashboard.</p> <p>Symantec Data Loss Prevention ships with executive summaries for Network, Endpoint, and Discover reports, and these are not customizable.</p> <p>You can create dashboards yourself, and customize them as desired.</p>
	<p>Custom</p> <p>Lists the shared reports that are associated with your current role. (Such reports appear only if you or other users in your current role have created them.)</p>
	<p>Network</p> <p>Lists the network incident reports.</p>
	<p>Endpoint</p> <p>Lists the Endpoint incident reports. Endpoint reports include incidents such as Endpoint Block and Endpoint Notify incidents.</p> <p>Incidents from Endpoint Discover are included in Discover reports.</p>
	<p>Discover</p> <p>Lists Network Discover and Endpoint Discover incident reports.</p> <p>The folder risk report displays file share folders ranked by prioritized risk. The risk score is based on the relevant information from the Symantec Data Loss Prevention incidents plus the information from the VML Management Server.</p>

Claim 1	Symantec Enterprise Cloud
	<div data-bbox="604 277 1472 342"> <p>Cloud Applications and API Appliance Lists Cloud Applications and API Appliance reports.</p> </div> <hr/> <div data-bbox="604 399 1860 464"> <p>Users The User List lists the data users in your organization. The User Risk Summary lists all users with their associated Email and Endpoint incidents.</p> </div> <hr/> <div data-bbox="594 540 1850 646"> <p>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/Incidents/managing-and-reporting-incidents/about-incident-reports-vont_0016-d336e1260.html)</p> </div>

an alerting component	<h2>About Endpoint Prevent response rules in different locales</h2> <p>Last Updated May 3, 2024</p> <p>You can create different endpoint response rule notifications that are specific to the locale of an endpoint. A locale refers to the system locale setting in the operating system of the endpoint.</p> <p>For example, you create response rule notifications in English, French, or Japanese. If a user's locale is specified as Japanese, the Japanese-language version of the notification appears on the user's screen. If a different user with a French locale violates the same policy, the French-language version of the notification appears.</p> <p>The Enforce Server lets you specify multiple user notifications. However, the first language that is specified is the default language. You cannot delete the default language response notification. You can add or delete any notification or language that is not specified as the default language. At installation, the default language is set to whichever language is set as the Enforce Server language. If the language you want is unsupported, the Enforce Server tries to display the English-language notification.</p> <p>For example, you have a Japanese-locale endpoint and a Vietnamese-locale endpoint. The Vietnamese locale is not a supported locale. If a violation occurs on the Japanese-locale computer, the Enforce Server displays the Japanese notification. If no Japanese notification is available, the Enforce Server displays the default-language notification. If the Vietnamese-locale computer violates a policy, the Enforce Server displays the English notification because no Vietnamese notification is possible. If the English notification is unavailable, the Enforce Server displays the default-language notification.</p> <p>If the first language you add is not supported on the endpoint, that language cannot be considered the default language. The endpoint must contain the specific language details to consider a language as the default language. Although the text of the notification appears in the unsupported language, the notification window buttons and title bar appear in the default locale of the Enforce Server.</p> <p>If you want to define an unsupported language as the default language, you must select Other as the first language. This Other label removes all other languages in the list. Use the Endpoint configuration options to modify the text of the pop-up window labels. You cannot specify other language responses if you select the Other option. The Other setting displays that language notification on every endpoint, regardless of the system locale of the endpoints.</p>
-----------------------	---

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="596 266 1850 375">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/how-to-implement-endpoint-prevent/about-endpoint-prevent-response-rules-in-different-locales.html)</p> <h2 data-bbox="596 396 1713 505">Configuring the Endpoint Prevent: Notify action</h2> <p data-bbox="596 526 926 558">Last Updated May 3, 2024</p> <p data-bbox="596 597 1871 695">The Endpoint Prevent: Notify response rule action displays an on-screen notification to the endpoint user when the user attempts to copy or send a sensitive file. You can provide a reason for the notification as well as options for the endpoint user to give a justification for the action.</p> <p data-bbox="596 716 940 748">About response rule actions</p> <p data-bbox="596 764 1304 797">This response rule action is available for Endpoint Prevent.</p> <p data-bbox="596 834 1850 899">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/response-rules-2/configuring-the-endpoint-prevent-notify-action.html)</p>

Claim 1	Symantec Enterprise Cloud
a policy database,	<p data-bbox="604 289 1787 347">About policy creation for Endpoint Prevent</p> <p data-bbox="604 363 924 394">Last Updated May 3, 2024</p> <p data-bbox="604 435 1885 532">Endpoint Prevent policies execute DCM and VML conditions locally on the endpoint. An Endpoint Prevent policy contains a response rule that creates a real-time user interaction. The user interaction either blocks a file transfer or notifies the user of a policy violation. These notifications are then attached to the incident.</p> <p data-bbox="604 553 1812 651">Endpoint policies also differ as to where the detection occurs. Detection for EDM and DGM policies is performed on the Endpoint Server. Detection for DCM and IDM policies is performed directly by the Symantec DLP Agent.</p> <p data-bbox="604 672 1793 703">The response rules Block, Notify, and User Cancel are performed only by the Symantec DLP Agent.</p> <p data-bbox="604 724 1881 854">Because detection for EDM, and DGM policies is performed on the Endpoint Server, the detection takes more time and uses more bandwidth. Extra time and bandwidth are required because file contents are sent to the Endpoint Server for detection. When an agent performs detection for IDM and DCM policies, it only sends incidents to the Endpoint Server.</p> <p data-bbox="596 881 1864 987">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-policy-creation-for-endpoint-prevent.html</p> <p data-bbox="604 1011 1507 1070">Creating an Endpoint Discover scan</p> <p data-bbox="604 1081 898 1112">Last Updated May 3, 2024</p> <p data-bbox="604 1146 1722 1206">To create an Endpoint Discover scan, you set up an Endpoint Discover target. Later you configure the target meet your scanning requirements.</p> <p data-bbox="604 1227 1780 1317">The Endpoint Discover target can also be configured to scan specific locations on endpoints. The scan can use filters to target local drives, file types, or folders to find policy violations. For example, the fixed drive or the My Documents folder in Windows can be configured as a filter.</p>

Claim 1	Symantec Enterprise Cloud
	https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/creating-an-endpoint-discover-scan.html
a user database,	<h2 data-bbox="604 418 932 472">User Groups</h2> <p data-bbox="604 488 911 521">Last Updated May 3, 2024</p> <p data-bbox="604 553 1787 618">You define User Groups on the Enforce Server. User Groups contain user identity information that you populate by synchronizing the Enforce Server with a group directory server (Microsoft Active Directory).</p> <p data-bbox="604 634 1787 699">You must have server administrator privileges to define User Groups. You must define the User Groups before you synchronize users.</p> <p data-bbox="604 716 1808 813">Once you define a User Group, you populate it with users, groups, and business units from your directory server. After the user group is populated, you associate it with the User/Sender and Recipient detection rules or exceptions. The policy only applies to members of that User Group.</p> <p data-bbox="604 829 1850 894"> https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/user-groups.html </p>

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="604 272 1209 326">Manage and add users</h2> <p data-bbox="604 344 936 375">Last Updated June 18, 2024</p> <p data-bbox="604 412 1793 443">The System > Login Management > DLP Users screen lists all the active user accounts in the system.</p> <p data-bbox="604 462 1268 493">For each user account, the following information is listed:</p> <ul data-bbox="615 511 1478 634" style="list-style-type: none"> • User Name – The name the user enters to log on to the Enforce Server • Email – The email address of the user • Access – The role(s) in which the user is a member <p data-bbox="604 652 1824 683">Assuming that you have the appropriate privileges, you can add, edit, or delete user accounts as follows:</p> <ul data-bbox="615 701 1713 914" style="list-style-type: none"> • Add a new user account, or modify an existing one. Click Add to begin adding a new user to the system. Click anywhere in a row or the pencil icon (far right) to view and edit that user account. Configuring user accounts • Click the red X icon (far right) to delete the user account; a dialog box confirms the deletion. <div data-bbox="663 969 732 997" data-label="Section-Header">Note</div> <div data-bbox="657 1011 1696 1042" data-label="Text"> <p>The Administrator account is created on install and cannot be removed from the system.</p> </div> <div data-bbox="657 1131 732 1161" data-label="Section-Header">Note</div> <div data-bbox="657 1177 1814 1242" data-label="Text"> <p>When you delete a user account, you also delete all private saved reports that are associated with that user.</p> </div>

Claim 1	Symantec Enterprise Cloud
	https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/Manage-the-Enforce-Server/managing-users-and-rules/manage-and-add-users-v27499097-d297e4727.html
a meta database	<h2 data-bbox="617 412 1654 467">Enabling endpoint metadata detection</h2> <p data-bbox="617 483 999 516">Last Updated February 16, 2024</p> <p data-bbox="617 555 1272 587">By default metadata extraction is disabled for endpoints.</p> <p data-bbox="617 604 1079 636">To enable endpoint metadata extraction</p> <ol data-bbox="617 652 1806 1058" style="list-style-type: none"> 1. Log on to the Enforce Server administration console as a system administrator. 2. Navigate to the System > Agents > Agent Configuration screen for the endpoint server you want to enable metadata extraction. 3. Create a new endpoint configuration for metadata detection, or select the default configuration. <a data-bbox="659 831 1407 863" href="#">Create a separate endpoint configuration for metadata detection 4. Select the Advanced Agent Settings tab. 5. Locate property <code>Detection.ENABLE_METADATA.str</code> in the list. 6. Enter the value on for this property to enable metadata extraction. 7. Click Save and Apply to save the configuration change. <p data-bbox="596 1091 1852 1237"> https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-data-loss-prevention-policies-v27576413-d327e9/supported-file-formats-for-metadata-extraction-v77411276-d327e136440/enabling-endpoint-metadata-detection-v80023038-d327e136628.html </p>

Claim 1	Symantec Enterprise Cloud									
	<h2>Creating an Endpoint Discover scan</h2> <p>Last Updated May 3, 2024</p> <p>To create an Endpoint Discover scan, you set up an Endpoint Discover target. Later you configure the target meet your scanning requirements.</p> <p>The Endpoint Discover target can also be configured to scan specific locations on endpoints. The scan can use filters to target local drives, file types, or folders to find policy violations. For example, the fixed drive or the My Documents folder in Windows can be configured as a filter.</p> <p>Steps to configure scan settings for an Endpoint Discover scan target</p> <table><tr><th>Step</th><th>Description</th><th>More information</th></tr><tr><td>1</td><td>Configure a new Endpoint Discover target.</td><td>Go to the Manage > Discover Scanning > Discover Targets screen and click New Target, Endpoint File System. Creating a new Endpoint Discover target</td></tr><tr><td>2</td><td>Configure the incremental or full scan.</td><td>You set this information on the General tab when you configure the new target. About Endpoint Discover incremental scanning About Endpoint Discover full scanning</td></tr></table>	Step	Description	More information	1	Configure a new Endpoint Discover target.	Go to the Manage > Discover Scanning > Discover Targets screen and click New Target, Endpoint File System . Creating a new Endpoint Discover target	2	Configure the incremental or full scan.	You set this information on the General tab when you configure the new target. About Endpoint Discover incremental scanning About Endpoint Discover full scanning
Step	Description	More information								
1	Configure a new Endpoint Discover target.	Go to the Manage > Discover Scanning > Discover Targets screen and click New Target, Endpoint File System . Creating a new Endpoint Discover target								
2	Configure the incremental or full scan.	You set this information on the General tab when you configure the new target. About Endpoint Discover incremental scanning About Endpoint Discover full scanning								

Claim 1	Symantec Enterprise Cloud	
	<p>3 Configure the targeted endpoints.</p>	<p>You set this information on the Targeting tab when you configure the new target.</p> <p>About scanning targeted endpoints</p>
	<p>4 Add <u>location, file size, date, and file type</u> filters to the Endpoint Discover target.</p>	<p>You enter this information on the Filters tab when you configure the new target.</p> <p>About Endpoint Discover filters</p>
	<p>5 Configure the scan idle timeout and max scan duration settings.</p>	<p>You set this information on the Advanced tab when you configure the new target.</p> <p>Configuring Endpoint Discover scan timeout settings</p>
	<p>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/creating-an-endpoint-discover-scan.html)</p>	

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="604 302 1730 358">Guidelines for authoring Endpoint policies</h2> <p data-bbox="604 375 915 407">Last Updated May 3, 2024</p> <p data-bbox="604 448 1850 675">Symantec Data Loss Prevention uses a two-tiered detection architecture to analyze activity on endpoints. Detection occurs either directly on DLP Agents or on the Endpoint Servers as required. Endpoint Servers can perform all types of detection, such as Exact Data Matching (EDM), Indexed Document Matching (IDM), and Directory Group Matching (DGM). Agents can perform Described Content Matching (DCM) and Indexed Document Matching (IDM). Symantec Data Loss Prevention <u>can detect locally on keywords, regular expressions, and data identifiers.</u> It must send input content to the Endpoint Server to detect on exact data fingerprints or indexed document fingerprints.</p> <p data-bbox="596 708 1850 808">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/guidelines-for-authoring-endpoint-policies.html</p>

Claim 1	Symantec Enterprise Cloud
and a settings database,	<p>Agent settings</p> <p>Last Updated May 3, 2024</p> <p>The Settings tab is divided into the following sections:</p> <ul style="list-style-type: none"> • Server Communication Server Communication settings • Inspection Content Size Increasing the Inspection Content Size • Resource Consumption on the Endpoint Host Resource Consumption on the Endpoint Host settings • Resource Consumption for Endpoint Discover Scans Resource Consumption for Endpoint Discover Scans settings • File Recovery Area Location File Recovery Area Location settings • LiveUpdate Enabling LiveUpdate in Agent Configurations • Safe Mode Safe Mode settings • Cloud Storage Cloud Storage settings • Printer/Fax Printer/Fax settings • Proxy Agent proxy settings • Microsoft Information Protection Microsoft Information Protection settings • Browser Extension Enablement Reminder Browser Extension Enablement Reminder • SEP Intensity Level About the SEP Intensive Protection file reputation service <p>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/adding-and-editing-agent-configurations/agent-settings.html.)</p>

Claim 1	Symantec Enterprise Cloud
the forensic computing platform further comprising at least one endpoint	<h2 data-bbox="621 293 1304 350">About Endpoint Discover</h2> <p data-bbox="621 367 932 396">Last Updated May 3, 2024</p> <p data-bbox="621 436 1860 532">Endpoint Discover detects sensitive data on your desktop or your laptop endpoints. It consists of at least one Endpoint Server and at least one Symantec DLP Agent that runs on an endpoint. You can have many Symantec DLP Agents connected to a single Endpoint Server. Symantec DLP Agents:</p> <ul data-bbox="630 553 1535 724" style="list-style-type: none"> • Detect sensitive data in the endpoint file system. • Collect data on that activity. • Send incidents to the Endpoint Server. • Send the data to the associated Endpoint Server for analysis, if necessary. <p data-bbox="598 764 1848 833">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/getting-started/introducing/about-endpoint-discover.html</p>

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="613 272 1871 383">About discovering and preventing data loss on endpoints</p> <p data-bbox="613 402 926 431">Last Updated May 3, 2024</p> <p data-bbox="613 472 1808 534">To use Endpoint Discover or Endpoint Prevent features, you need to deploy DLP Agents and Endpoint Servers.</p> <p data-bbox="613 557 1864 683">Endpoint Prevent and Endpoint Discover both apply Data Loss Prevention policies to protect your sensitive or at-risk data. Sensitive or at-risk data can include credit card numbers or names, addresses, and identification numbers. You can configure both of these products to recognize and protect the files that contain sensitive data.</p> <p data-bbox="613 706 1079 735">See About Endpoint Prevent monitoring.</p> <p data-bbox="613 756 1850 919">Endpoint Prevent stops sensitive data from moving off endpoints and supported virtual desktops. For example, Endpoint Prevent can stop a file that contains credit card numbers from being transferred to eSATA, USB, or FireWire-connected media. Endpoint Prevent stops sensitive the files from being transferred to network shares. And Endpoint Prevent can monitor and prevent data from being transferred to applications you specify.</p> <p data-bbox="613 940 1871 1200">Endpoint Discover scans the internal hard drives of an endpoint to identify stored confidential data so steps can be taken to inventory, secure, or relocate this data. It enables high-performance, parallel scanning of tens of thousands of endpoints with minimal system effect. Each DLP Agent can scan approximately 5 GB/hr. Users can set up Endpoint Discover scans to use multiple Endpoint Servers to increase performance and scan availability. Endpoint Discover can automatically quarantine confidential files either locally to a folder on the Windows endpoint computer (including to an encrypted folder) or remotely to a folder on the network. Endpoint features provides description of these features as well as where to find additional information.</p> <p data-bbox="613 1221 1850 1282">You can configure agent settings, group agents, set response rules, check agent health, and troubleshoot agents.</p> <p data-bbox="598 1320 1850 1388">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints.html</p>

Claim 1	Symantec Enterprise Cloud
<p>and modules to detect, classify, delete, encrypt, and redact data stored on the at least one endpoint</p>	<p>“modules to detect [and] classify . . . data stored on the at least one endpoint”</p> <p>About Endpoint Prevent monitoring</p> <p>Last Updated May 3, 2024</p> <p>Endpoint Prevent policies detect and block confidential information moving from Windows and macOS endpoints or virtual desktops in your organization. The Endpoint Server either pushes policies to DLP Agents or applies policies directly to files that are sent from the DLP Agents. Depending on the type of policy that you create, the policy is applied either by the DLP Agents directly or by the Endpoint Server. When DLP Agents or Endpoint Servers detect an activity that violates a policy rule, an incident is generated. You can review and remediate the incidents that display in the endpoint incident list.</p> <p>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-endpoint-prevent-monitoring.html)</p>

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="611 267 1507 321">About Endpoint Discover Scanning</h2> <p data-bbox="611 337 909 365">Last Updated May 3, 2024</p> <p data-bbox="611 406 1801 557">Endpoint Discover scans the local drive of endpoints to find any currently existing files that violate your policies. Endpoint Discover scans all local drives on your endpoints. For example, if your computer has two physical local drives installed, Endpoint Discover scans both local drives for any files that violate your policies. Endpoint Discover does not scan those drives that are mounted through a network or removable media such as eSATA drives, flash drives, or SD cards.</p> <p data-bbox="611 576 1755 636">You can use Endpoint Discover to scan all the endpoints in an organization and scan only the specified endpoints in an organization. Endpoint Discover supports Windows, macOS, and Linux endpoints.</p> <div data-bbox="611 670 1808 870"> <p data-bbox="632 690 695 714">Note</p> <p data-bbox="632 734 1751 831">Beginnign with Symantec Data Loss Prevention 15.0, Two Tier Detection (TTD) is not supported. However, even if a Two Tier Detection request is generated for DLP Agent versions earlier than 15.0, Endpoint Server ignores these agents, and does not perform two-tier detection.</p> </div> <p data-bbox="611 904 1801 1149">To start or stop a scan that is configured for an Endpoint Server, the DLP Agent must be connected to the Endpoint Server. If the DLP Agent is not connected to the Endpoint Server, the scan starts when it reconnects to the Endpoint Server. A scan is only complete when all of the endpoints have completed the scan. If one endpoint is disconnected from the Endpoint Server, the scan cannot complete until that endpoint reconnects or the scan times out. If an endpoint is disconnected after a scan has started, the endpoint continues the scan offline and communicates the status after it reconnects to the Endpoint Server. If the endpoint remains disconnected and exceeds a configured timeout period, the scan reports a timeout status.</p> <p data-bbox="611 1170 1791 1230">In a load-balanced environment, select all of the Endpoint Servers that connect to a load balancer. So that when endpoints connect to any of these Endpoint Servers, the endpoints receive the same scan details.</p> <p data-bbox="611 1250 1776 1339">All incidents are stored in the Agent Store until the computer is reconnected to the Endpoint Server. If the Agent Store exceeds the specified size limit, the scan pauses until the Agent reconnects to the Endpoint Server and transfers the incidents.</p>

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="596 266 1873 370">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-discovering-and-preventing-data-loss-on-endp-v98548126-d294e27/about-scanning-v16318536-d294e26629.html)</p> <h2 data-bbox="611 381 1646 492">About the SEP Intensive Protection file reputation service</h2> <p data-bbox="611 509 921 537">Last Updated May 3, 2024</p> <p data-bbox="611 579 1856 706">Symantec Data Loss Prevention integrates with Symantec Endpoint Protection (beginning with SEP 14.0.1) to enable a new channel of Endpoint monitoring: SEP Intensive Protection. By leveraging the application reputation information that SEP provides, the DLP Agent can dynamically monitor applications and can prevent potentially harmful applications from accessing sensitive files on the endpoint.</p> <p data-bbox="611 727 1843 854">You can configure the DLP Agent to monitor applications of a specified reputation threshold established by SEP. The application reputations can be Malicious, Suspicious, or Unproven. You can use these reputations as conditions in response rules you create, so Symantec Data Loss Prevention can take different actions based on specific reputations for multiple endpoint channels and policies.</p> <p data-bbox="611 875 1667 902">The DLP Agent obtains the application reputation information from SEP in one of two ways:</p> <ul data-bbox="621 924 1808 1063" style="list-style-type: none"> <li data-bbox="621 924 1808 1019">• If the SEP agent is installed on the endpoint, the SEP agent sends the information to the DLP Agent directly. If the SEP agent does not have information, the DLP Agent gets information from the SEP Intensive Protection file reputation service in the Symantec cloud. <li data-bbox="621 1036 1671 1063">• If the SEP agent is not installed, the SEP Cloud sends the information to the DLP Agent. <p data-bbox="611 1084 1856 1144">The incident details for dynamic application monitoring include the application reputation. You can also filter incidents by SEP intensity level categories.</p> <p data-bbox="611 1166 1843 1226">The dynamic monitoring of applications based on reputation requires only an Endpoint Prevent license. No additional license is needed.</p> <p data-bbox="596 1247 1885 1351">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-the-sep-intensive-protection-file-reputation-service.html)</p>

Claim 1	Symantec Enterprise Cloud
	<p>“module[] to . . . delete . . . data stored on the at least one endpoint”</p> <p>Configuring the Endpoint Discover: Quarantine File action</p> <p>Last Updated May 3, 2024</p> <p>The Endpoint Discover: Quarantine File response rule action removes a file containing sensitive information from a non-secure location and places it in a secure location.</p> <p>This response rule action is specific to Endpoint Discover incidents. This response rule is not applicable to two-tiered detection methods requiring a Data Profile.</p> <p>If you use multiple endpoint response rules in a single policy, make sure that you understand the order of precedence for such rules.</p> <p>About response rule action execution priority</p> <p>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/response-rules-2/configuring-the-endpoint-discover-quarantine-file-action.html#v39343965)</p>

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="617 272 1507 316">Configuring the Delete Data-at-Rest action</p> <p data-bbox="617 329 856 354">Last Updated May 3, 2024</p> <p data-bbox="617 383 1581 431">The Delete Data-at-Rest action deletes sensitive data in the following cloud applications through the Cloud Detection Service:</p> <ul data-bbox="617 448 888 542" style="list-style-type: none"> • Dropbox • Gmail • Microsoft Office 365 Email <p data-bbox="617 558 1010 583">To configure the Delete Data-at-Rest action</p> <ol data-bbox="617 594 1255 618" style="list-style-type: none"> 1. Configure a response rule at the Configure Response Rule screen. <p data-bbox="646 634 894 659">Configuring response rules</p> <ol data-bbox="617 675 1199 699" style="list-style-type: none"> 2. Add the Delete Data-at-Rest action type from the Actions list. <p data-bbox="646 716 1104 740">The system displays the Delete Data-at-Rest field.</p> <p data-bbox="646 743 953 768">Configuring response rule actions</p> <ol data-bbox="617 784 978 808" style="list-style-type: none"> 3. Click Save to save the configuration. <p data-bbox="646 824 863 849">Manage response rules</p> <p data-bbox="598 870 1843 935">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/response-rules-2/configuring-the-delete-data-at-rest-action.html#v119247645)</p> <p data-bbox="598 959 1535 984">“module[] to . . . encrypt . . . data stored on the at least one endpoint”</p>

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="611 272 1751 380">Configuring the Endpoint Prevent: Encrypt action</h2> <p data-bbox="611 402 921 430">Last Updated May 3, 2024</p> <p data-bbox="611 472 1829 532">The Endpoint Prevent: Encrypt response rule action automatically encrypts a sensitive file and displays a notification when a user attempts to do any of the following:</p> <ul data-bbox="611 553 1845 976" style="list-style-type: none"> <li data-bbox="611 553 1845 683">• Transfer a sensitive file to a removable storage device A user can copy a sensitive file to the removable storage device through Windows Explorer, Command Line, or PowerShell. The DLP Agent blocks the Save As operation for an encrypted file on a removable storage device. <li data-bbox="611 699 1845 797">• Transfer a sensitive file to a cloud storage application Examples of commonly used cloud storage applications are Box, Google Drive, Microsoft OneDrive, and so on. <li data-bbox="611 813 1845 976">• Upload a sensitive file or folder with encrypted files with browsers using HTTPS on Windows endpoints When a user uploads a sensitive file or folder using a browser, the DLP Agent blocks a user action and automatically encrypts the file with an .html extension and replaces the original file at the source location. A user is then prompted to upload this encrypted file or folder using the browser to protect sensitive information. <p data-bbox="611 997 1713 1024">The maximum supported file size for the Endpoint Prevent: Encrypt response action is 150 MB.</p> <p data-bbox="611 1045 938 1073">About response rule actions</p> <p data-bbox="611 1094 1814 1122">For information about the Endpoint Prevent: Encrypt response rule action, Response rule best practices</p> <p data-bbox="611 1143 1850 1268">When a violation is detected, the DLP Agent encrypts the file, the data transfer completes, and an incident is created. You can provide a reason for the notification as well as options for the endpoint user to enter a justification for the action. This response rule action is available for Endpoint Prevent on Windows and Mac endpoints.</p> <p data-bbox="611 1300 1845 1370">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/response-rules-2/configuring-the-endpoint-prevent-encrypt-action.html)</p>

About cloud storage application monitoring

Last Updated May 3, 2024

Endpoint cloud storage application monitoring provides monitor and prevent support for cloud file sync and share applications. You can access cloud storage application monitoring settings on the **System > Agents > Global Application Monitoring** screen.

If an endpoint user updates content in the files that a cloud application syncs, the cloud application attempts to upload the file to the cloud service. If a user adds sensitive content, Symantec Data Loss Prevention prevents the file from uploading to the cloud.

If you use a block response rule in the policy, Symantec Data Loss Prevention creates a Cloud Storage incident, and sensitive content is quarantined on the endpoint. The endpoint user can restore the previous file version from the configured recovery location where the file is saved indefinitely. [File Recovery Area Location settings](#)

(<https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-endpoint-prevent-monitoring/about-cloud-storage-application-monitoring.html>)

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="611 289 1430 342">About Endpoint FlexResponse</h2> <p data-bbox="611 362 919 391">Last Updated May 3, 2024</p> <p data-bbox="611 431 1839 526">Symantec Data Loss Prevention provides a set of response rule actions that you can specify to remediate an incident. These provided actions include logging, sending an email, blocking an end-user action, notifying a user, and other responses.</p> <p data-bbox="611 545 1833 672">You can also use Endpoint FlexResponse plug-ins to provide additional response actions. These plug-ins contain custom instructions for remediation actions that are executed on endpoints. Endpoint FlexResponse rules are only applicable to Automated Response rules. You cannot create Endpoint FlexResponse rule actions for Smart Response rules.</p> <p data-bbox="611 691 1860 850">Symantec Data Loss Prevention customers can contact Symantec or Symantec partners to obtain Endpoint FlexResponse plug-ins. In addition, developers with a knowledge of the Python programming language can create custom Endpoint FlexResponse plug-in scripts using a Symantec-provided API. These custom remediation actions can include encryption, applying Digital Rights Management (DRM), or redacting confidential information.</p> <div data-bbox="611 889 1860 1045"> <p data-bbox="632 911 695 940">Note</p> <p data-bbox="632 959 1766 1024">The DLP Agent supports Python 3.8. Make sure that your custom Endpoint FlexResponse plug-in scripts have been updated to work with Python 3.8.</p> </div> <p data-bbox="611 1081 1854 1276">You use the Endpoint FlexResponse utility to deploy Endpoint FlexResponse plug-ins on endpoints in your Symantec Data Loss Prevention deployment where you require Endpoint FlexResponse actions. You can deploy the plug-ins manually using the Endpoint FlexResponse utility, or you can use system management software (SMS) to distribute the utility and deploy the plug-ins. After you deploy an Endpoint FlexResponse plug-in on an endpoint, you use the Enforce Server administration console to add an Endpoint: FlexResponse action to a response rule, and then you add the response rule to an active policy.</p>

Claim 1	Symantec Enterprise Cloud
	<p>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-endpoint-flexresponse.html)</p> <p>“module[] to . . . redact data stored on the at least one endpoint”</p>

Configuring the Redact Data-in-Motion action

Last Updated May 3, 2024

The **Redact Data-in-Motion** action redacts sensitive data in applications through the Cloud Detection Service or API Detection for Developer Apps Appliance.

You can configure a message for your users to inform them why the sensitive data was redacted. The message appears in the message parameter of the detection response.

To configure the Redact Data-in-Motion action

1. Configure a response rule at the **Configure Response Rule** screen.

[Configuring response rules](#)

2. Add the **Redact Data-in-Motion** action type from the **Actions** list.

The system displays the **Redact Data-in-Motion** field.

[Configuring response rule actions](#)

3. Configure the **Redact Data-in-Motion** parameter.

[Redact Data-in-Motion configuration parameter](#)

4. Click **Save** to save the configuration.

[Manage response rules](#)

Redact Data-in-Motion configuration parameter

Parameter	Description
Message	Enter a user-facing message for the Redact Data-in-Motion action in the message field. These details are returned in the message parameter of the detection result.

(<https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/response-rules-2/configuring-the-redact-data-in-motion-action.html>)

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="611 289 1430 342">About Endpoint FlexResponse</h2> <p data-bbox="611 362 919 391">Last Updated May 3, 2024</p> <p data-bbox="611 431 1839 526">Symantec Data Loss Prevention provides a set of response rule actions that you can specify to remediate an incident. These provided actions include logging, sending an email, blocking an end-user action, notifying a user, and other responses.</p> <p data-bbox="611 545 1833 672">You can also use Endpoint FlexResponse plug-ins to provide additional response actions. These plug-ins contain custom instructions for remediation actions that are executed on endpoints. Endpoint FlexResponse rules are only applicable to Automated Response rules. You cannot create Endpoint FlexResponse rule actions for Smart Response rules.</p> <p data-bbox="611 691 1860 850">Symantec Data Loss Prevention customers can contact Symantec or Symantec partners to obtain Endpoint FlexResponse plug-ins. In addition, developers with a knowledge of the Python programming language can create custom Endpoint FlexResponse plug-in scripts using a Symantec-provided API. These custom remediation actions can include encryption, applying Digital Rights Management (DRM), or redacting confidential information.</p> <div data-bbox="611 889 1860 1045"> <p data-bbox="632 911 695 940">Note</p> <p data-bbox="632 959 1766 1024">The DLP Agent supports Python 3.8. Make sure that your custom Endpoint FlexResponse plug-in scripts have been updated to work with Python 3.8.</p> </div> <p data-bbox="611 1081 1854 1276">You use the Endpoint FlexResponse utility to deploy Endpoint FlexResponse plug-ins on endpoints in your Symantec Data Loss Prevention deployment where you require Endpoint FlexResponse actions. You can deploy the plug-ins manually using the Endpoint FlexResponse utility, or you can use system management software (SMS) to distribute the utility and deploy the plug-ins. After you deploy an Endpoint FlexResponse plug-in on an endpoint, you use the Enforce Server administration console to add an Endpoint: FlexResponse action to a response rule, and then you add the response rule to an active policy.</p>

Claim 1	Symantec Enterprise Cloud
	https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-endpoint-flexresponse.html)
<p>the forensic computing platform causing the following steps to occur when executing computer instructions stored in a memory of the cloud control server: receiving, by one of the modules of the forensic computing platform from the at least one endpoint, a meta log associated with a first file, the meta log comprising: a first file name, data element tags comprising indicators that data types are included in the first file, one or more of a date created, date deleted, or date modified, and an endpoint ID;</p>	<h2 data-bbox="611 402 1629 451">About document metadata detection</h2> <p data-bbox="611 472 999 500">Last Updated February 16, 2024</p> <p data-bbox="611 545 1871 670">In addition to file content and subfile extraction, Symantec Data Loss Prevention supports metadata extraction for many file formats. File format metadata is data about a file that is stored as file properties. By default metadata extraction is disabled because it can lead to false positives. Used properly, metadata detection can enhance the accuracy of your content-based policy rules.</p> <p data-bbox="611 695 1860 885">For example, consider a business that uses Microsoft Office templates for their Word, Excel, and PowerPoint documents. The business applies Microsoft OLE metadata properties in the form of keywords to each template. The business has enabled metadata extraction and deployed keyword policies to match on metadata keywords. These policies can detect keywords in documents that are derived from the templates. The business also has the flexibility to use policy exceptions to avoid generating incidents if certain metadata keywords are present.</p> <p data-bbox="596 906 1871 1040"> https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-data-loss-prevention-policies-v27576413-d327e9/supported-file-formats-for-metadata-extraction-v77411276-d327e136440/about-document-metadata-detection-v77411550-d327e136433.html) </p>

Collecting Server Logs and Configuration Files

Last Updated June 27, 2024

Use the **Collection** tab of the **System > Servers and Detectors > Logs** screen to collect log files and configuration files from one or more Symantec Data Loss Prevention servers. You can collect files from a single detection server or from all detection servers, the Enforce Server computer and Network Discover Cluster. You can limit the collected files to only those files that were last updated in a specified range of dates.

Following are the details for log collection for all the Detection Servers (except Network Discover Cluster) and Network Discover Cluster:

Details of log collection

Location/Targets	Description
All Detection Servers, except Network Discover Cluster	The Enforce Server administration console stores all log and configuration files that you collect in a single ZIP file on the Enforce Server computer. If you retrieve files from multiple Symantec Data Loss Prevention servers, each server's files are stored in a separate subdirectory of the ZIP file.
Network Discover Cluster	For Network Discover Cluster log collection, when you select the Operational Logs, Debug and Trace Logs , or Configuration Files checkbox, the File Path and Credentials fields are displayed. Enter the file share path and credentials for a file share folder where you want to upload the cluster log files. You must have read and write permissions for this file share folder. The cluster logs are uploaded to this file share and they are not stored on the Enforce Server. The data node and all the worker nodes in the cluster upload their logs to this file share.

Claim 1	Symantec Enterprise Cloud						
	<p data-bbox="615 274 882 305">File types for collection</p> <table border="1" data-bbox="615 321 1864 1157"> <thead> <tr> <th data-bbox="615 337 726 368">File type</th><th data-bbox="1041 337 1176 368">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="615 427 827 457">Operational Logs</td><td data-bbox="1041 427 1843 735"> <p data-bbox="1041 427 1843 621">Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files to troubleshoot any problems in the way the software integrates with other components of your system.</p> <p data-bbox="1041 643 1843 735">For example, you can use operational log files to verify that a Network Prevent for Email Server communicates with a specific MTA on your network.</p> </td></tr> <tr> <td data-bbox="615 794 892 824">Debug and Trace Logs</td><td data-bbox="1041 794 1850 1157"> <p data-bbox="1041 794 1850 1157">Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain a Symantec Data Loss Prevention installation. However, Symantec Support may ask you to provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary.</p> </td></tr> </tbody> </table>	File type	Description	Operational Logs	<p data-bbox="1041 427 1843 621">Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files to troubleshoot any problems in the way the software integrates with other components of your system.</p> <p data-bbox="1041 643 1843 735">For example, you can use operational log files to verify that a Network Prevent for Email Server communicates with a specific MTA on your network.</p>	Debug and Trace Logs	<p data-bbox="1041 794 1850 1157">Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain a Symantec Data Loss Prevention installation. However, Symantec Support may ask you to provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary.</p>
File type	Description						
Operational Logs	<p data-bbox="1041 427 1843 621">Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files to troubleshoot any problems in the way the software integrates with other components of your system.</p> <p data-bbox="1041 643 1843 735">For example, you can use operational log files to verify that a Network Prevent for Email Server communicates with a specific MTA on your network.</p>						
Debug and Trace Logs	<p data-bbox="1041 794 1850 1157">Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain a Symantec Data Loss Prevention installation. However, Symantec Support may ask you to provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary.</p>						

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="625 293 850 326">Configuration Files</p> <p data-bbox="1045 293 1717 358">Use the Configuration Files option to retrieve both logging configuration files and server feature configuration files.</p> <p data-bbox="1045 375 1808 505">Logging configuration files define the overall level of logging detail that is recorded in server log files. Logging configuration files also determine whether specific features or subsystem events are recorded to log files.</p> <p data-bbox="1045 521 1808 586">You can modify many common logging configuration properties by using the presets that are available on the Configuration tab.</p> <p data-bbox="1045 602 1843 764">If you want to update a logging configuration file by hand, use the Configuration Files checkbox to download the configuration files for a server. You can modify individual logging properties using a text editor and then use the Configuration tab to upload the modified file to the server.</p> <p data-bbox="1045 781 1459 813">Configuring server logging behavior</p> <p data-bbox="1045 829 1843 1154">The Configuration Files option retrieves the active logging configuration files and also any backup log configuration files that were created when you used the Configuration tab. This option also retrieves server feature configuration files. Server feature configuration files affect many different aspects of server behavior, such as the location of a syslog server or the communication settings of the server. You can collect these configuration files to help diagnose problems or verify server settings. However, you cannot use the Configuration tab to change server feature configuration files. You can only use the tab to change logging configuration files.</p>

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="617 272 756 302">Agent Logs</p> <p data-bbox="1037 272 1839 467">Use the Agent Logs option to collect DLP agent service and operational log files from an Endpoint Prevent detection server. This option is available only for Endpoint Prevent servers. To collect the DLP Agent logs, you must have already pulled the log files from individual agents to the Endpoint Prevent detection server using a Pull Logs action.</p> <p data-bbox="1037 488 1839 586">Use the Agent List screen to select individual agents and pull selected log files to the Endpoint Prevent detection server. Then use the Agent Logs option on this page to collect the log files.</p> <p data-bbox="1037 607 1839 769">When the logs are pulled from the endpoint, they are stored on the Endpoint Server in an unencrypted format. After you collect the logs from the Endpoint Server, the logs are deleted from the Endpoint Server and are stored only on the Enforce Server. You can only collect logs from one endpoint at a time.</p> <p data-bbox="596 802 1839 906">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/15-8/about-managing-servers-v15599809-d297e16684/collecting-server-logs-and-configuration-files-v33480324-d297e24269.html</p>

DLP Agent Logs

Last Updated February 16, 2024

DLP Agent logs contain service and operational data for every DLP Agent. Each DLP Agent has multiple components that are logged. The amount of information that is logged can be configured by setting the log level for each DLP Agent component. After the log level for an DLP Agent component has been configured, the log can be collected and sent to Symantec Support. Symantec Support can use the log to troubleshoot a problem or to improve performance for a Symantec Data Loss Prevention Endpoint installation.

See [Setting the log levels for an Endpoint Agent](#).

(<https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/maintaining-the-system/understanding-underlying-system-resources-v15258948-d363e192/about-dlp-agent-logs-v75416710-d294e15012.html>)

Gathering endpoint device IDs for removable devices

Last Updated February 16, 2024

You add device metadata information to the Enforce Server and create one or more policy detection methods that detect or except the specific device instance or class of device. The system supports the regular expression syntax for defining the metadata. The system displays the device metadata at the **Incident Snapshot** screen during remediation.

Creating and modifying endpoint device configurations

The metadata the system requires to define the device instance or device class is the **Device Instance ID**. On Windows you can obtain the "Device Instance Id" from the Device Manager.

In addition, Symantec Data Loss Prevention provides DeviceID.exe for devices attached to Windows endpoints and DeviceID for devices attached to Mac endpoints. You can use these utilities to extract Device Instance ID strings and device regex information. These utilities also report what devices the system can recognize for detection. These utilities are available with the Enforce Server installation files.

Note

The Device Instance ID is also used by Symantec Endpoint Protection.

To obtain the Device Instance ID (on Windows)

1. Right-click **My Computer**.
2. Select **Manage**.
3. Select the **Device Manager**.
4. Click the plus sign beside any device to expand its list of device instances.
5. Double-click the device instance. Or, right-click the device instance and select **Properties**.
6. Look in the **Details** tab for the **Device Instance Id**.
7. Use the ID to create device metadata expressions.

(<https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-data-loss-prevention-policies-v27576413-d327e9/configuring-endpoint-event-detection-conditions-v85252962-d327e125553/gathering-endpoint-device-ids-for-removable-device-v42760780-d327e126068.html>)

Detecting data loss

Last Updated May 3, 2024

Symantec Data Loss Prevention detects data from virtually any type of message or file, any user, sender, or recipient, wherever your data or endpoints exist. You can use Data Loss Prevention to detect both the content and the context of data within your enterprise. You define and manage your detection policies from the centralized, Web-based Enforce Server administration console.

(<https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/detecting-data-loss.html>)

Content that can be detected

Last Updated May 3, 2024

Symantec Data Loss Prevention detects data and document content, including text, markup, presentations, spreadsheets, archive files and their contents, email messages, database files, designs and graphics, multimedia files, image-based forms and more. For example, the system can open a compressed file and scan a Microsoft Word document within the compressed file for the keyword "confidential." If the keyword is matched, the detection engine flags the message as an incident.

Content-based detection is based on actual content, not the file itself. A detection server can detect extracts or derivatives of protected or described content. This content may include sections of documents that have been copied and pasted to other documents or emails. A detection server can also identify sensitive data in a different file format than the source file. For example, if a confidential Word file is fingerprinted, the detection engine can match the content emailed in a PDF attachment.

(<https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/detecting-data-loss/content-that-can-be-detected.html>)

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="611 272 1310 326">Files that can be detected</h2> <p data-bbox="611 347 919 375">Last Updated May 3, 2024</p> <p data-bbox="611 418 1871 545">Symantec Data Loss Prevention recognizes many types of files and attachments based on their context, including file type, file name, and file size. Symantec Data Loss Prevention identifies over 300 types of files, including word-processing formats, multimedia files, spreadsheets, presentations, pictures, encapsulation formats, encryption formats, and others.</p> <p data-bbox="611 568 1871 662">For file type detection, the system does not rely on the file extension to identify the file type. For example, the system recognizes a Microsoft Word file even if a user changes the file extension to .txt. In this case the detection engine checks the binary signature of the file to match its type.</p> <p data-bbox="611 690 1871 797">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/detecting-data-loss/files-that-can-be-detected.html</p>
<p data-bbox="205 834 548 976">storing the meta log in the cloud control server of the forensic computing platform;</p>	<h2 data-bbox="611 834 1619 888">About document metadata detection</h2> <p data-bbox="611 909 919 937">Last Updated May 3, 2024</p> <p data-bbox="611 980 1850 1107">In addition to file content and subfile extraction, Symantec Data Loss Prevention supports metadata extraction for many file formats. File format metadata is data about a file that is stored as file properties. By default metadata extraction is disabled because it can lead to false positives. Used properly, metadata detection can enhance the accuracy of your content-based policy rules.</p> <p data-bbox="611 1130 1850 1321">For example, consider a business that uses Microsoft Office templates for their Word, Excel, and PowerPoint documents. The business applies Microsoft OLE metadata properties in the form of keywords to each template. The business has enabled metadata extraction and deployed keyword policies to match on metadata keywords. These policies can detect keywords in documents that are derived from the templates. The business also has the flexibility to use policy exceptions to avoid generating incidents if certain metadata keywords are present.</p>

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="596 266 1881 370">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/supported-file-formats-for-metadata-extraction/about-document-metadata-detection.html)</p> <h2 data-bbox="632 412 854 467">Log files</h2> <p data-bbox="632 483 936 509">Last Updated May 3, 2024</p> <p data-bbox="632 552 1829 610">Symantec Data Loss Prevention provides a number of different log files that record information about the behavior of the software. Log files fall into these categories:</p> <ul data-bbox="640 633 1839 821" style="list-style-type: none"> • Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files to troubleshoot any problems in the way the software integrates with other components of your system. For example, you can use operational log files to verify that a Network Prevent for Email Server communicates with a specific MTA on your network. <p data-bbox="672 841 919 867">Operational Log Files</p> <ul data-bbox="640 889 1850 1114" style="list-style-type: none"> • Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain an Symantec Data Loss Prevention installation. However, Symantec Support may ask you to provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary. <p data-bbox="672 1117 863 1143">Debug Log Files</p> <ul data-bbox="640 1166 1850 1390" style="list-style-type: none"> • Installation log files record information about the Symantec Data Loss Prevention installation tasks that are performed on a particular computer. You can use these log files to verify an installation or troubleshoot installation errors. Installation log files reside in the following locations: <ul data-bbox="688 1279 1755 1390" style="list-style-type: none"> – installldir\SymantecDLP\.install4j\installation.log stores the installation log for Symantec Data Loss Prevention. – installldir\oracle_home\admin\protect\ stores the installation log for Oracle.

Claim 1	Symantec Enterprise Cloud
	https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/maintaining-the-dlp-system/log-files.html

Claim 1	Symantec Enterprise Cloud		
	Operational log files		
	Log file name	Description	Server
	agentmanagement_webservices_access_0.log	Logs successful and failed attempts to access the Agent Management API web service.	Enforce Server
	agentmanagement_webservices_soap_0.log	Logs the entire SOAP request and response for most requests to the Agent Management API web Service.	Enforce Server
	boxmonitor_operational_0.log	<p>The BoxMonitor process oversees the detection server processes that pertain to that particular server type.</p> <p>For example, the processes that run on Network Monitor are file reader and packet capture.</p> <p>The BoxMonitor log file is typically very small, and it shows how the application processes are running.</p>	All detection servers
detection_operational_0.log	The detection operation log file provides details about how the detection server configuration and whether it is operating correctly.	All detection servers	

	detection_operational_trace_0.log	<p>The detection trace log file provides details about each message that the detection server processes. The log file includes information such as:</p> <ul style="list-style-type: none"> • The policies that were applied to the message • The policy rules that were matched in the message • The number of incidents the message generated. 	All detection servers
	machinelearning_training_operational_0.log	This log records information about the tasks, logs, and configuration files called on startup of the VML training process.	Enforce Server
	manager_operational_0.log.	Logs information about the Symantec Data Loss Prevention manager process, which implements the Enforce Server administration console user interface.	Enforce Server
	monitorcontroller_operational_0.log	Records a detailed log of the connections between the Enforce Server and all detection servers. It provides details about the information that is exchanged between these servers including whether policies have been pushed to the detection servers or not.	Enforce Server

Claim 1	Symantec Enterprise Cloud		
	SmtpPrevent_operational0.log	This operational log file pertains to SMTP Prevent only. It is the primary log for tracking the health and activity of a Network Prevent for Email system. Examine this file for information about the communication between the MTAs and the detection server.	SMTP Prevent detection servers
	WebPrevent_Access0.log	This access log file contains information about the requests that are processed by Network Prevent for Web detection servers. It is similar to web access logs for a proxy server.	Network Prevent for Web detection servers
	WebPrevent_Operational0.log	This operational log file reports on the operating condition of Network Prevent for Web, such as whether the system is up or down and connection management.	Network Prevent for Web detection servers
	(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/maintaining-the-dlp-system/log-files/operational-log-files.html)		

analyzing, by the analytic component, the indicators of the data element tags of the first file based on a configured setting and criteria;

About discovering and preventing data loss on endpoints

Last Updated May 3, 2024

To use Endpoint Discover or Endpoint Prevent features, you need to deploy DLP Agents and Endpoint Servers.

Endpoint Prevent and Endpoint Discover both apply Data Loss Prevention policies to protect your sensitive or at-risk data. Sensitive or at-risk data can include credit card numbers or names, addresses, and identification numbers. You can configure both of these products to recognize and protect the files that contain sensitive data.

See [About Endpoint Prevent monitoring](#).

Endpoint Prevent stops sensitive data from moving off endpoints and supported virtual desktops. For example, Endpoint Prevent can stop a file that contains credit card numbers from being transferred to eSATA, USB, or FireWire-connected media. Endpoint Prevent stops sensitive the files from being transferred to network shares. And Endpoint Prevent can monitor and prevent data from being transferred to applications you specify.

Endpoint Discover scans the internal hard drives of an endpoint to identify stored confidential data so steps can be taken to inventory, secure, or relocate this data. It enables high-performance, parallel scanning of tens of thousands of endpoints with minimal system effect. Each DLP Agent can scan approximately 5 GB/hr. Users can set up Endpoint Discover scans to use multiple Endpoint Servers to increase performance and scan availability. Endpoint Discover can automatically quarantine confidential files either locally to a folder on the Windows endpoint computer (including to an encrypted folder) or remotely to a folder on the network. [Endpoint features](#) provides description of these features as well as where to find additional information.

You can configure agent settings, group agents, set response rules, check agent health, and troubleshoot agents.

	Endpoint features		
	Feature	Description	Additional information
	Agent configuration	You can select which endpoint egress channels to monitor, and you can optimize monitoring by choosing appropriate filters. You can also configure server-agent communication bandwidth limits and agent resource consumption.	About agent configurations
	Agent groups	You use agent groups to send agent configurations to groups of agents.	About agent groups
	Agent health and management	You can review DLP Agent health and complete troubleshooting and management tasks.	About Symantec DLP Agent administration
	Global application monitoring	You can configure this feature to monitor applications for CD/DVD burning, IM, email, or HTTP/S clients.	About global application monitoring
	FlexResponse	You can create response rules that automatically remediate incidents.	About Endpoint FlexResponse
	Endpoint tools	You use Endpoint tools to complete various maintenance tasks on the endpoint, like shutting down watchdog services, inspecting the agent database, and restarting Mac agents.	Endpoint Tools

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="598 266 1848 334">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints.html)</p> <h2 data-bbox="611 342 1617 402">About Endpoint Prevent monitoring</h2> <p data-bbox="611 418 934 451">Last Updated May 3, 2024</p> <p data-bbox="611 492 1860 695">Endpoint Prevent policies detect and block confidential information moving from Windows and macOS endpoints or virtual desktops in your organization. The Endpoint Server either pushes policies to DLP Agents or applies policies directly to files that are sent from the DLP Agents. Depending on the type of policy that you create, the policy is applied either by the DLP Agents directly or by the Endpoint Server. When DLP Agents or Endpoint Servers detect an activity that violates a policy rule, an incident is generated. You can review and remediate the incidents that display in the endpoint incident list.</p> <p data-bbox="598 740 1887 842">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-endpoint-prevent-monitoring.html)</p> <h2 data-bbox="611 857 1640 917">Endpoint events that can be detected</h2> <p data-bbox="611 933 926 966">Last Updated April 5, 2024</p> <p data-bbox="611 1006 1883 1136">Symantec Data Loss Prevention lets you detect data loss violations at several endpoint destinations. These destinations include the local drive, CD/DVD drive, removable storage devices, network file shares, Windows Clipboard, printers and faxes, and application files. You can also detect protocol events on the endpoint for email (SMTP), Web (HTTP), and file transfer (FTP) traffic.</p> <p data-bbox="611 1157 1877 1255">For example, the DLP Agent (installed on each endpoint computer) can detect the copying of a confidential file to a USB device. Or, the DLP Agent can allow the copying of files only to a specific class of USB device that meets corporate encryption requirements.</p> <p data-bbox="598 1276 1848 1378">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0/about-data-loss-prevention-policies-v27576413-d327e9/detecting-data-loss-v15598681-d327e1049/endpoint-events-that-can-be-detected-v40065947-d327e1125.html)</p>

Claim 1	Symantec Enterprise Cloud								
	<div>Endpoint matching conditions</div> <div>Last Updated April 5, 2024</div> <div>Symantec Data Loss Prevention provides several conditions for matching endpoint events.</div> <div>Endpoint events that can be detected</div> <div>Endpoint matching conditions</div> <table><tr><th>Condition</th><th>Description</th></tr><tr><td>Protocol or Endpoint Monitoring</td><td>Match endpoint messages transmitted using a specified transport protocol or when data is moved or copied to a particular destination. Introducing endpoint event detection Configuring the Endpoint Monitoring condition</td></tr><tr><td>Endpoint Device Class or ID</td><td>Match endpoint events occurring on specified hardware devices. Introducing endpoint event detection Configuring the Endpoint Device Class or ID condition</td></tr><tr><td>Endpoint Location</td><td>Match endpoint events depending if the DLP Agent is on or off the corporate network. Introducing endpoint event detection Configuring the Endpoint Location condition</td></tr></table> <div>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0/about-data-loss-prevention-policies-v27576413-d327e9/policy-matching-conditions-v40499624-d327e1698/endpoint-matching-conditions-v41286484-d327e2045.html#v41286484)</div>	Condition	Description	Protocol or Endpoint Monitoring	Match endpoint messages transmitted using a specified transport protocol or when data is moved or copied to a particular destination. Introducing endpoint event detection Configuring the Endpoint Monitoring condition	Endpoint Device Class or ID	Match endpoint events occurring on specified hardware devices. Introducing endpoint event detection Configuring the Endpoint Device Class or ID condition	Endpoint Location	Match endpoint events depending if the DLP Agent is on or off the corporate network. Introducing endpoint event detection Configuring the Endpoint Location condition
Condition	Description								
Protocol or Endpoint Monitoring	Match endpoint messages transmitted using a specified transport protocol or when data is moved or copied to a particular destination. Introducing endpoint event detection Configuring the Endpoint Monitoring condition								
Endpoint Device Class or ID	Match endpoint events occurring on specified hardware devices. Introducing endpoint event detection Configuring the Endpoint Device Class or ID condition								
Endpoint Location	Match endpoint events depending if the DLP Agent is on or off the corporate network. Introducing endpoint event detection Configuring the Endpoint Location condition								

Claim 1	Symantec Enterprise Cloud
	<h2 data-bbox="617 293 1839 349">About Data Loss Prevention Policy Authoring</h2> <p data-bbox="617 367 926 394">Last Updated May 3, 2024</p> <p data-bbox="617 436 1875 500">Use Symantec Data Loss prevention policy authoring features to detect and prevent data loss. DLP provides seven key features that enable you to create policies that protect your organization from data loss.</p> <p data-bbox="617 521 1871 716">You implement policies to detect and prevent data loss. A Symantec Data Loss Prevention policy combines detection rules and response actions. If a policy rule is violated, the system generates an incident that you can report and act on. The policy rules that you implement are based on your information security objectives. The actions that you take in response to policy violations are based on your compliance requirements. The Enforce Server administration console provides an intuitive, centralized, web-based interface for authoring policies.</p> <p data-bbox="598 753 1848 816">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring.html</p>

determining, based on the indicators of the data element tags, a data classification associated with the first file comprised on the at least one endpoint;

About Endpoint reports

Last Updated February 16, 2024

Use incident reports to track and remediate incidents on your endpoints. Symantec Data Loss Prevention reports an incident when it detects data that matches the detection parameters of a policy rule. Such data may include specific file content, an email sender or recipient, attachment file properties, or many other types of information. Each piece of data that matches detection parameters is called a match, and a single incident may include any number of individual matches.

Reporting for Endpoint Discover is found under the Discover Reporting section. Endpoint Discover incidents are marked to distinguish them from other types of Discover incidents.

Reporting for Endpoint Prevent is found in the **Reports** tab of the Enforce Server.

You can view the following reports:

- Exec. Summary - Endpoint
- Incidents - All
- Incidents - New
- Policy Summary
- Status Summary
- Highest Offenders

If an incident is created that includes user justifications, those justifications are included in the report in the Incident snapshot section. For example, if a violation occurs that requires the user to enter the response User error, the incident report includes the text SPECIAL: User typed response: "User error".

If the user selects a pre-generated justification, the justification appears in the report. Justifications appear in the detailed report under the header Justifications.

Justifications and notifications are not compatible with Endpoint Discover, therefore no justifications appear in Endpoint Discover reports.

You can also create customized reports for Endpoint Discover and Prevent. However, if the user is not on the network at the time the justification is entered, the justification section of the incident snapshot remains empty.

Claim 1	Symantec Enterprise Cloud
	<p>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-discovering-and-preventing-data-loss-on-endp-v98548126-d294e27/managing-target-scans-v97535512-d294e27271/about-endpoint-reports-v15602064-d294e366.html)</p> <h2 data-bbox="606 412 1793 521">Configuring the Endpoint: MIP Classification action</h2> <p data-bbox="606 542 991 573">Last Updated February 16, 2024</p> <p data-bbox="606 613 1864 776">When MIP classification is enabled for supported applications in the agent configuration, the Endpoint: MIP Classification response action enables DLP Agents and the Enforce Server to suggest classification labels for Microsoft Office documents and outgoing emails in Microsoft Outlook that contain confidential information. Alternatively, DLP Agents can apply labels automatically when the Endpoint: MIP Classification response action is triggered.</p> <div data-bbox="627 813 1871 1073"> <p data-bbox="632 833 695 860">Note</p> <ul data-bbox="638 883 1864 1040" style="list-style-type: none"> <li data-bbox="638 883 1864 987">• MIP classification is available for outgoing emails in Microsoft Outlook only on Windows endpoints. If an email already has a label that enforces MIP encryption, DLP does not inspect the email again for classification. <li data-bbox="638 1003 1163 1040">• Labels are applied to the email body only. </div> <p data-bbox="606 1109 1770 1206">Regardless of whether a label is suggested to users or whether a label is applied automatically, the Endpoint: MIP Classification response action enables you to configure a pop-up notification that is displayed to users.</p> <p data-bbox="594 1242 1848 1344">(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-response-rules-v40462357-d339e11/Configuring-the-Endpoint--MIP-Classification-action-.html)</p>

Claim 1	Symantec Enterprise Cloud
<p>and predicting data breaches based on degree changes in data topology wherein as meta data is received and stored in the meta database the meta data is consumed by the analytics component which produces signals that are sent to the alerting component wherein a first signal may reflect a spike in user activity and wherein a second signal may reflect data of a specific classification that has leaked onto one or more endpoints.</p>	<div data-bbox="1577 305 1824 334">SOLUTION BRIEF</div> <div data-bbox="1068 394 1751 423">Customer-Focused Threat Prevention Innovations</div> <p data-bbox="1068 435 1818 688">Symantec software innovations are reshaping <i>threat prevention</i> strategies by driving a proactive approach to combat the modern tactics and techniques that attackers use today. Symantec Enterprise Cloud uses advanced artificial intelligence and machine learning to predict where the next attack might occur and block attacks before they are executed. Our threat prevention solution also provides insights into areas where attack vectors can be closed, eliminating these options from an attacker's tool chest. The combined effect of a reduced attack surface, enterprise-grade security controls, and our foundational Global Intelligence Network ensures that threat prevention is implemented with the highest levels of efficacy.</p> <p data-bbox="1068 711 1785 760">Key innovations for <i>threat prevention</i> within Symantec Enterprise Cloud include the following features:</p> <ul data-bbox="1068 781 1824 1273" style="list-style-type: none"> • Adaptive Protection – Reduces the attack surface by blocking trusted application behaviors often used by attackers to execute living-off-the-land attacks. Attackers are frequently successful when they use an organization's known applications to execute an attack because they can hide their activities. This analytic technology can customize blocking adaptations based on its ability to continuously learn which apps, tools, and OS behaviors are used in the customer's environment—and which are not used. Adaptive Protection automatically restricts unused behaviors to reduce the attack surface and protect the organization. This feature is transformative in blocking threats from entering the environment without affecting normal business operations. • Application Control – Discovers installed applications and their vulnerabilities, reputation and prevalence, and generates a risk score for addressing the security concerns associated with the broad use of <i>shadow IT</i>. Delivered with the risk score is a risk assessment, actionable insights, and smart recommendations for blocking or allowing an application to run. With Application Control, organizations can specify the apps they allow, and block the apps that are dangerous and unnecessary. <div data-bbox="669 462 928 518">DATA PROTECTION INNOVATIONS</div> <ul data-bbox="669 532 1010 1081" style="list-style-type: none"> • Generative AI Protection: Provide guardrails for users while enabling a productive and lower risk work environment • ZTNA Data Protection: Enforce Data Loss Prevention (DLP) policies against private resources and corporate assets in the cloud • Risk-Aware Policies: Create greater context for DLP policies so access and control can be adapted to users with higher risk scores • Fast File Scanning: Dramatic increases in the scan rates for large data repositories ensures that static data can be scanned regularly with new and updated DLP policies • Leading Edge Data Detection: New detection methods increase detection accuracy and reduce the rate of false positives <p data-bbox="598 1321 1505 1351">https://docs.broadcom.com/doc/threat-prevention-and-data-protection</p>

Claim 1	Symantec Enterprise Cloud
	<ul style="list-style-type: none">• Anomaly detection: Performs advanced statistical analysis on captured data to create a baseline of the organization's network traffic and user activity, then detects outliers based on numerical, linguistic, and information density analysis. Security Analytics alerts on anomalous behavior with a pivot to the Anomaly Investigation view to see when the anomaly occurred, how often, and which parts of the network were involved. <p>(https://docs.broadcom.com/doc/security-analytics-appliances-en)</p>

Claim 1	Symantec Enterprise Cloud						
	<div>Behavior-Based Incident Detectors</div> <div>Last Updated July 18, 2024</div> <div>The Symantec CloudSOC Detect app identifies threats based on behavior. For each Detector, you configure Confidence and Importance levels.</div> <div><table><tr><th>Behavior-based detector</th><th>Reports an incident when:</th></tr><tr><td>Anomalously large number of user actions</td><td><div>There is an unusually large volume of user actions such as:</div><ul style="list-style-type: none">• Copy• Edit• Open• Preview• Unshare• View instance (for example on AWS)<div>The Detector learns a profile for action volume for each user. It triggers an alert when a user performs a large number of actions uncharacteristic of their historical SaaS app usage.</div></td></tr><tr><td>Anomalously large download data</td><td><div>There is an unusually large amount of data downloaded for a given combination of user and SaaS application.</div><div>The Detector learns a profile for download volume for each user. It triggers an alert when a user downloads a large volume of data uncharacteristic of their historical SaaS app usage.</div></td></tr></table></div>	Behavior-based detector	Reports an incident when:	Anomalously large number of user actions	<div>There is an unusually large volume of user actions such as:</div> <ul style="list-style-type: none">• Copy• Edit• Open• Preview• Unshare• View instance (for example on AWS) <div>The Detector learns a profile for action volume for each user. It triggers an alert when a user performs a large number of actions uncharacteristic of their historical SaaS app usage.</div>	Anomalously large download data	<div>There is an unusually large amount of data downloaded for a given combination of user and SaaS application.</div> <div>The Detector learns a profile for download volume for each user. It triggers an alert when a user downloads a large volume of data uncharacteristic of their historical SaaS app usage.</div>
Behavior-based detector	Reports an incident when:						
Anomalously large number of user actions	<div>There is an unusually large volume of user actions such as:</div> <ul style="list-style-type: none">• Copy• Edit• Open• Preview• Unshare• View instance (for example on AWS) <div>The Detector learns a profile for action volume for each user. It triggers an alert when a user performs a large number of actions uncharacteristic of their historical SaaS app usage.</div>						
Anomalously large download data	<div>There is an unusually large amount of data downloaded for a given combination of user and SaaS application.</div> <div>The Detector learns a profile for download volume for each user. It triggers an alert when a user downloads a large volume of data uncharacteristic of their historical SaaS app usage.</div>						

Claim 1	Symantec Enterprise Cloud
	<p data-bbox="611 293 987 326">Anomalous variety of file types</p> <p data-bbox="1102 293 1688 326">A user accesses an unusual variety of file types.</p> <p data-bbox="1102 331 1881 565">The Detector learns the number of different types of files that each user interacts with on each individual cloud service. For instance, business analysts might primarily interact with a couple of file types on Google drive. It might be highly unusual if they started interacting with many more file types on Google drive. The learned profile changes over time as the user interacts with different number of file types.</p> <p data-bbox="1102 586 1881 755">The Detector does not evaluate the file's internal content, just the file type extension. To prevent users from getting around this detector, configure the file type mismatch detector to alert you if there are mismatches between the filename extension and true underlying file type.</p> <p data-bbox="596 771 1856 836">https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud/detect-home/understanding-detectors/behavior-based-incident-detectors.html</p>